

NOT FOR PUBLICATION

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA, :
: Cr. No. 14-287 (FLW)
Plaintiff, :
: **MEMORANUDM OPINION**
v. : **and ORDER**
:
MENDEL EPSTEIN, JAY :
GOLDSTEIN, DAVID ARYEH :
EPSTEIN, and :
BINYAMIN STIMLER, :
:
Defendants. :
:

WOLFSON, United States District Judge:

The Court has rendered a number of evidentiary decisions on the record in this criminal case, and recently, published a written opinion on the defenses and evidentiary issues relating to the Religious Freedom Restoration Act ("RFRA"), raised by defendants Rabbi Mendel Epstein, Rabbi Jay Goldstein ("Goldstein"), David Epstein and Rabbi Binyamin Stimler (collectively, "Defendants"). See *United States v. Epstein*, No. 14-287, 2015 U.S. Dist. LEXIS 34156 (D.N.J. Mar. 19, 2015). Included in the series of decisions on the record, the Court denied Goldstein's motion to exclude the Government's evidence on historical cell site location

information ("CSLI").¹ In this Opinion, this Court sets forth in detail its reasoning in denying that request.

Because I have extensively recounted the background facts of this case in my prior opinion, I will not repeat them here. See *Epstein*, 2015 U.S. Dist. LEXIS at *2-6. Suffice to say, Defendants are on trial for charges of conspiracy to commit kidnapping, attempted kidnapping, and kidnapping. As part of its evidence, the Government introduced information relating to historical cell site and other location data from Defendants' mobile telephones, which information was obtained by a court order pursuant to 18 U.S.C. § 2703(d).² Indeed, on October 30, 2014, under that statutory authority, a Magistrate Judge granted the Government's application to acquire CSLI from wireless providers of Defendants' cell phones.

An overview of CSLI is helpful. Mobile telephone service providers operate a system of towers to receive and transmit signals from mobile phones. When a mobile telephone user places or receives a call, the telephone sends an electronic signal to the nearest tower. Service providers generate and retain records which identify the

¹ I note that all other defendants joined in Goldstein's motion in this regard.

² To be clear, in this case, the Government is not seeking to introduce any prospective cell site data.

particular tower to which a user's telephone was connected at the beginning and end of each call. In that regard, CSLI identifies, albeit not precisely, the location where a call is made or received.

On this motion, Defendants argue that the suppression of the CSLI in this case is appropriate because the Government obtained the information through a § 2703(d) order, not a Fourth Amendment warrant based on probable cause. Defendants reason that while § 2703(d) permits disclosure of CSLI upon a showing to a magistrate judge that the information is relevant to an ongoing investigation or prosecution, the Supreme Court's decisions in *Riley v. California*, 134 S.Ct. 2473 (2014) and *United States v. Jones*, 132 S.Ct. 945 (2012), render § 2703(d) constitutionally infirm, and that a warrant based upon a showing of probable cause is necessary to obtain such information. On the record, I gave my reasons for rejecting Defendants' contention. In this written Opinion, I elaborate more fully on my analysis.

Title II of the Electronic Communications Privacy Act, the Stored Communications Act ("SCA"), governs requests for access to stored records, including historical cell site data or CSLI. Under the SCA, the government may obtain an order to access such records "only if the government entity

offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). While this provision permits the government to obtain CSLI data with the lower "reasonable grounds" standard than a showing of probable cause, in this circuit, § 2703(d) has been held constitutional. See *In re United States For An Order Directing Provider Of Electronic Communication Service To Disclose Records*, 620 F.3d 304 (3d Cir. 2010) ("*In re Electronic Communication*").

In *In re Electronic Communication*, the Third Circuit was confronted with the issue whether warrantless collection of historical cell site data, pursuant to a § 2703(d) order, violates a criminal defendant's Fourth Amendment rights. After analyzing the statutory framework, the Third Circuit found that "CSLI from cell phone calls is obtainable under a § 2703(d) order and that such an order does not require the traditional probable cause determination. Instead, the standard is governed by the text of § 2703(d), [i.e., the reasonable grounds standard].'" *Id.* at 313 (quoting 18 U.S.C. § 2703(d)).

Here, notwithstanding the Third Circuit's decision in this regard, Defendants submit that the recent Supreme Court cases of *Riley* and *Jones* altered the Fourth Amendment landscape involving stored electronic data, and thus, Defendants argue, *In re Electronic Communication* is no longer the controlling precedent on this issue. While the Third Circuit has not had the occasion to review its decision in *In re Electronic Communication* in light of *Riley* and *Jones*, I, nevertheless, do not find that these Supreme Court decisions change the outcome here.

In *Riley*, the question before the Supreme Court was whether the search-incident-to-arrest doctrine allows the government to search an arrestee's cell phone without a warrant. Ultimately, the Court held that police must obtain a search warrant before searching a cell phone's contents. *Riley*, 134 S. Ct. at 2485, 2488. In so holding, the Supreme Court reasoned that "[m]odern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse." *Id.* And, because a modern cell phone has the capability to store an immense amount of data about an individual's private life, Fourth Amendment concerns would be implicated. *Id.* at 2489, 2495.

As the Fifth Circuit in *U.S. v. Guerrero*, 768 F.3d 351 (5th Cir. 2014), observed, "although the issues in *Riley* . . . implicate a broader theme concerning the application of the Fourth Amendment to modern technology," the *Riley* Court based its decision on the rationale that the defendant in that case indisputably had an expectation of privacy in the contents of his personal cell phone. *Guerrero*, 768 F.3d at 359. The issue in this case involves the different question of whether a cell phone owner has a reasonable expectation of privacy in information held by a "third party" service provider. See *Id.* The *Riley* Court recognized that these are different issues when it distinguished the seminal "third party" doctrine decision in *Smith v. Maryland*, 442 U.S. 735 (1979). The Court explained:

The Government relies on *Smith v. Maryland*, which held that no warrant was required to use a pen register at telephone company premises to identify numbers dialed by a particular caller. The Court in that case, however, concluded that the use of a pen register was not a "search" at all under the Fourth Amendment. There is no dispute here that the officers engaged in a search of [defendant's] cell phone. Moreover, call logs typically contain more than just phone numbers; they include any identifying information that an individual might add, such as the label "my house" in [defendant's] case.

Riley, 134 S.Ct. at 2492-93. Simply put, *Riley* did not address the constitutionality of utilizing § 2703(d) to

obtain historical cell site location data from *third-party* cell phone providers.

I also do not find that the Supreme Court's decision in *U.S. v. Jones* probative in my analysis here. In that case, the Supreme Court concluded that the warrantless attachment of a Global-Positioning-System ("GPS") tracking device to an individual's vehicle and subsequent use of that device to monitor the vehicle's movements on a public street violated the Fourth Amendment. See *Jones*, 132 S.Ct. at 948-49. However, in so holding, the Court reasoned that the physical intrusion involved in attaching the GPS tracking device to the individual's vehicle constituted a search within the meaning of the Fourth Amendment. 132 S.Ct. at 949. In that respect, the Court rejected the government's position that defendant Jones had no reasonable expectation of privacy in the area of the vehicle accessed by the government's agents.

Id. Based on the Supreme Court's reasoning and its application of the Fourth Amendment, *Jones* is not dispositive of the issues here. Nothing announced in *Jones* would "invalidate the authorization of Congress under § 2703(d) to obtain records concerning electronic communication from a third party provider of electronic communication service." *Martinez*, 2014 U.S. Dist. LEXIS 153485 at *12.

Indeed, the seizure of historical cell site location information under § 2703(d) does not involve physical intrusion upon Defendants' property or any real time tracking information. Thus, *Jones* and *Riley* are distinguishable from this case because the facts here do not concern the search or seizure of a cell phone, or the content of any communication. Rather, the subscriber information provided by the third party cell phone service providers was cell site location data from their historical databases. Indeed, these are business records created and maintained by the service providers, which are not entitled to protection under Defendants' Fourth Amendment rights. See *Smith*, 442 U.S. at 742 (finding that a pen register installed on telephone company property to record the telephone numbers dialed by the defendant did not constitute a search within the meaning of the Fourth Amendment, because the defendant did not have a reasonable expectation of privacy regarding the number dialed on his phone; a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.).³ A vast majority

³ To be fair, I recognize that there are at least two district courts in the country that have decided differently, see *U.S. v. Cooper*, No. 13-693, 2015 U.S. Dist. LEXIS 25935 (N.D. Cal. Mar. 2, 2015) and *In re Application of United States for an Order Authorizing the Release of Historical Cell-Site Info.*, 809 F. Supp. 2d 113, 116

of the courts across the country take the same view. See, e.g., *U.S. v. Dorsey*, No. 14-328, 2015 U.S. Dist. LEXIS 23693, at *22-23 (C.D. Cal. Feb. 23, 2015); *U.S. v. Martinez*, No. 13-3560, 2014 U.S. Dist. LEXIS 153485 (S.D. Cal. Oct. 28, 2014); *U.S. v. Moreno-Nevarez*, No. 13-0841, 2013 U.S. Dist. LEXIS 143900 (S.D. Cal. Oct. 2, 2013) (upholding the constitutionality of § 2703(d) and noting that "even if the statute were to be held unconstitutional, the good faith exception to the warrant requirement would apply"); *U.S. v. Salas*, No. 11-0354, 2013 U.S. Dist. LEXIS 116551 (E.D. Cal. Aug. 16, 2013) ("With regard to the argument applying the . . . Fourth Amendment to cell site location information, there is no reasonable expectation of privacy since such records are in the hands of third parties."); *U.S. v. Rigmaiden*, No. 08-814, 2013 U.S. Dist. LEXIS 65633 (D. Ariz. May 8, 2013) ("Courts have rejected . . . arguments that historical cell-site records cannot be obtained under the SCA."); *U.S. v. Ruby*, No. 12-1073, 2013 U.S. Dist. LEXIS 18997 (S.D. Cal. Feb. 12, 2013) (similar);

(E.D.N.Y. 2011). However, based on my reasoning here, I do not find those decisions to be persuasive. And, while the Eleventh Circuit in *U.S. v. Davis*, 754 F.3d 1205, 1215 (11th Cir. 2014), found that historical cell site data is within the subscriber's reasonable expectation of privacy, that decision has since been vacated, pending rehearing *en banc*, see *Davis*, 573 Fed. Appx. 925 (11th Cir. 2014). Therefore, *Davis* has no precedential or persuasive value.

U.S. v. Davis, No. 10-339, 2011 U.S. Dist. LEXIS 56002 (D. Or. May 24, 2011) ("It is well established that a reasonable expectation of privacy extends only to the content of telephone conversations, not to records that indicate that the conversations occurred. Basic subscriber data which identifies a call's origination, destination, duration, and time of call enjoy no privacy protection because the data is incidental to the use of the telephone, and contains no content information." (citations omitted)); *U.S. v. Herevia*, No. 13-639, 2014 U.S. Dist. LEXIS 133142 (D. Md. Sep. 23, 2014); *U.S. v. Rogers*, No. 13-952, 2014 U.S. Dist. LEXIS 145980 (N.D. Ill. Oct. 9, 2014)(notwithstanding *Riley* and *Jones*, "an individual user has no reasonable expectation of privacy in" CSLI, and therefore, "it is unnecessary for the government to obtain a search warrant.").

As a final note, however, jurisprudence involving cellular telephones and related technology is evolving, and "[i]t may be that the 'technology is different' rationale that led the *Riley* Court to treat an arrestee's cell phone differently from his wallet will one day lead the [Supreme] Court to treat historical cell site data in the possession of a cellphone provider differently from a pen register in the possession of a pay phone operator." See *Guerrero*, 768 F.3d at 358 (explaining that the Supreme Court may very well

weigh in on this issue). But, absent any contrary direction from a higher court -- particularly the Third Circuit -- I conclude that the Government may constitutionally acquire subscriber information and historical cell site data pursuant to a § 2703(d) order by providing specific and articulable facts showing that there are reasonable grounds to believe that the records sought, are relevant and material to an ongoing criminal investigation.

Utilizing such a standard, I find that the Government's application in obtaining a § 2703(d) order from the Magistrate Judge was sufficient under the statute. In the application, for example, the Government sought CSLI data from AT&T, a cellular service provider. The Government described the investigation into the kidnapping conspiracy in great detail. Indeed, the application outlined the criminal scheme that was under investigation at the time and identified five targets, including defendant Goldstein. Importantly, the Government stated that those targets were subscribers of the cellular telephone service and identified the cell phone numbers for those targets. Further, the application requested an order seeking the disclosure of CSLI regarding the cellular phone service of four of the targets, including Goldstein, on the ground that "there are reasonable grounds to believe that" such information would

be "relevant and material to an ongoing criminal investigation," and will assist the investigators "identify the location of the alleged participants in the scheme during the time periods when the alleged kidnappings and attempted kidnappings occurred." See Application, Part I. I find that the articulated and specific facts contained in the application met the requirements of § 2703(d).

Furthermore, even assuming that the current standard under § 2703(d), i.e., reasonable grounds, is unconstitutional, the CSLI evidence at issue would still be admissible under the good faith exception pursuant to *U.S. v. Leon*, 468 U.S. 897 (1984). In *Leon*, the Supreme Court held "that the exclusionary rule does not apply when the police conduct a search in 'objectively reasonable reliance' on a warrant later held invalid." *Davis v. United States*, 131 S. Ct. 2419, 2428 (2011). "If the purpose of the exclusionary rule is to deter unlawful police conduct, then evidence obtained from a search should be suppressed only if it can be said that the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional under the Fourth Amendment." *Leon*, 468 U.S. at 919 (citing *United States v. Peltier*, 422 U.S. 531, 542, (1975)). "For exclusion to be appropriate,

the deterrence benefits of suppression must outweigh the rule's heavy costs." *Davis*, 131 S. Ct. at 2422.

In other words, the good faith exception applies to "an officer acting in objectively reasonable reliance on a statute" authorizing a warrantless search or seizure of evidence. *Illinois v. Krull*, 480 U.S. 340, 350-56 (1987). In fact, such an exception applies in the context of this case, which concerns an order for cell site information obtained under Section 2703(d). See *United States v. Serrano*, No. 13-58, 2014 U.S. Dist. LEXIS 81478, at *7 (S.D.N.Y. Jun. 10, 2014); *United States v. Mack*, No. 13-54, 2014 U.S. Dist. LEXIS 159686, at *4 (D. Conn., Nov. 13, 2014); *United States v. Muniz*, No. 12-221, 2013 U.S. Dist. LEXIS 12162, at *6-8 (S.D. Tex. Jan. 29, 2013).

To be clear, evidence should be suppressed only if: (1) the magistrate has abandoned his detached and neutral role, (2) the officers were dishonest or reckless in preparing their affidavit, or (3) the officers could not have "harbored an objectively reasonable belief that probable cause existed." *Leon*, 468 U.S. at 926.

Here, because the vast majority of courts have upheld the constitutionality of § 2703(d), and because the § 2703(d) order was supported by affidavits containing at least some grounds for suspicion, the officers involved in

obtaining the order at issue could, at the very least, have reasonably relied on the Magistrate Judge's issuance of that order. While the Magistrate Judge's order involved, arguably, an unsettled question of law – namely, whether the SCA allows the government to obtain cell site data absent a showing of probable cause – there is nothing in the record to suggest that the Magistrate Judge "abandoned [his or her] detached and neutral role" in arriving at the ultimate decision. In addition, this Court cannot find any evidence -- nor is there any suggestion by Defendants -- that the Government was dishonest or misleading in its applications for cell site data. Nor can the Court, given the legal discussion above, conclude that "a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization." *Leon*, 468 U.S. at 922. This Court, therefore, finds that the good faith exception applies in this case even if § 2703(d) is found to be unconstitutional under the Fourth Amendment. See *Moreno-Nevarez*, No. 13-841, 2013 U.S. Dist. LEXIS 143900 (S.D. Cal. Oct. 1, 2013) (law enforcement officers relying on § 2703(d) order issued by neutral magistrate would qualify for good faith exception); *United States v. Graham*, 846 F. Supp. 2d 384, 405-06 (D. Md. 2012) ("Even if the government's acquisition of historical cell site location records in this

case had been in violation of the Defendants' Fourth Amendment rights, it obtained those records in good faith reliance on a constitutional statute and valid Orders issued by [neutral judicial officers]."'); *United States v. Jones*, 908 F. Supp. 2d 203, 214-16 (D.D.C. 2012) (similar).⁴

Accordingly, for the reasons stated on the record and herein, and for good cause shown,

IT IS on this 13th day of April, 2015,

ORDERED that Defendants' motion to suppress CSLI evidence is **DENIED**.

SO ORDERED.

/s/ Freda L. Wolfson
Freda L. Wolfson, U.S.D.J.

⁴ Indeed, even though the Eleventh Circuit in its since-vacated opinion in *Davis* decided contrary to the majority of cases cited herein that the Fourth Amendment does protect historical cell site data, that court nonetheless applied the good faith exception and declined to suppress the CSLI evidence in that case. See *Davis*, 754 F.3d at 1218.